



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/679,916	10/05/2000	Robert E. Ellingson	13481.1US01	8813
23552	7590	06/23/2006	EXAMINER	
MERCHANT & GOULD PC P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 06/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/679,916	ELLINGSON, ROBERT E.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 13 April 2006.

2a)  This action is FINAL.                    2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

4)  Claim(s) 1-14 and 27-34 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5)  Claim(s) \_\_\_\_\_ is/are allowed.

6)  Claim(s) 1-14 and 27-34 is/are rejected.

7)  Claim(s) \_\_\_\_\_ is/are objected to.

8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 05 October 2000 is/are: a)  accepted or b)  objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3)  Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5)  Notice of Informal Patent Application (PTO-152)  
6)  Other: \_\_\_\_\_.  
\_\_\_\_\_

## DETAILED ACTION

1. This is in response to the amendment filed on 13 April 2006.
2. Claims 1-14 and 27-34 are pending in the application.
3. Claims 1-14 and 27-34 have been rejected.
4. Claims 15-26 have been cancelled.

### *Response to Arguments*

5. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 1-4, 7, 8, 10-14 and 27-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Flitcroft et al U.S. Patent No. 6,636,833 B1.**

As to claim 1, Flitcroft et al discloses a method of obstructing identity crimes, the method comprising:

obtaining a list of at least two identity verifiers, each identity verifier to be used for no more than one transaction [column 9 line 64 to column 10 line 18];

linking the list of identity verifiers to at least one numerical identifier associated with a registered user, the registered user selected from the group consisting of persons and entities [column 11, lines 15-19];

providing the list of identity verifiers to the registered user [column 9 line 64 to column 10 line 18];

enabling the registered user to provide security information to be associated with one of the identity verifiers, the information pertaining to an intended transaction [column 9 line 64 to column 10 line 18];

receiving a numerical identifier from a requesting party, the requesting party having obtained the numerical identifier from a transaction initiator claiming to be associated with the numerical identifier [column 27, lines 15-50];

receiving an identity verifier from the requesting party, the requesting party having obtained the numerical identifier from a transaction initiator claiming to be associated with the numerical identifier [column 27, lines 15-50];

determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier [column 27, lines 15-50]; and

communicating information to the requesting party indicating whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier [column 27, lines 15-50]; and

sending to the requesting party any security message associated with the received identity verifier to enable the requesting party to compare the security

message with a transaction being conducted by the transaction initiator [column 27, lines 15-50].

As to claim 2, Flitcroft et al discloses that the communicating information step signals that the received identity verifier has not been used before and is within the list of identity verifiers linked to the received numerical identifier by sending a verification transaction identifier to the requesting party [column 9 line 64 to column 10 line 18].

As to claims 3 and 32, Flitcroft et al discloses the method further comprising:

(a) determining whether the identity verifier received from the requesting party has been used before [column 9 line 64 to column 10 line 18]; and

(b) communicating information to the requesting party signaling whether the identity verifier has been used before [column 9 line 64 to column 10 line 18].

As to claim 4, Flitcroft et al suggests archiving the identity verifier and the verification transaction identifier [column 9 line 64 to column 10 line 18].

As to claims 7, 8, 10 and 31, Flitcroft et al discloses that the at least one numerical identifier is a drivers license number, bank account number or a credit card number [column 9 line 64 to column 10 line 18].

As to claims 11 and 30, Flitcroft et al discloses receiving a uniqueness suffix and wherein determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier further comprises determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier and the received uniqueness suffix [column 9 line 64 to column 10 line 18].

As to claim 12, Flitcroft et al suggest discloses receiving a numerical identifier. Flitcroft et al discloses receiving an identity verifier and communicating information to the requesting party are performed by voice communications over a phone line [abstract].

As to claim 13, Flitcroft et al discloses that receiving a numerical identifier, receiving an identity verifier and communicating information to the requesting party are performed through electronic communication through a wide area network [abstract].

As to claim 14, Flitcroft et al discloses a method of determining whether an identity verifier is required to be submitted in a particular transaction, the method comprising the steps of:

- (a) obtaining a list of at least two identity verifiers, each identity verifier to be used for no more than one transaction [column 9 line 64 to column 10 line 18];
- (b) linking the list of identity verifiers to at least one unique numerical identifier wherein the numerical identifier is associated with a registered user selected from a group consisting of persons and entities [column 11, lines 15-19];
- (c) creating categories of transactions [column 6 line 66 to column 7 line 16];
- (d) receiving instructions from the registered user designating the categories of transactions that require an identity verifier and designating the categories of transactions that do not require an identity verifier [column 6 line 66 to column 7 line 16];

- (e) receiving a numerical identifier from a requesting party, the requesting party having obtained the numerical identifier from a transaction initiator claiming to be associated with the numerical identifier [column 27, lines 15-50];
- (f) receiving information from the requesting party specifying the type of transaction occurring [column 16, lines 43-62];
- (g) determining whether the transaction requires the use of an identity verifier [column 16, lines 43-62]; and
- (h) communicating information to the requesting party wherein the information communicated indicates whether an identity verifier is required for the specified transaction [column 16, lines 43-62].

As to claim 27, Flitcroft et al discloses a method of obstructing identity crimes, the method comprising:

associating a plurality of identity verifiers with a registered user, each of the identity verifiers to be used for a single transaction [column 9 line 64 to column 10 line 18];

receiving from the registered user at least one security message, each security message corresponding to one of the plurality of identity verifiers [column 11, lines 15-19];

associating each security message provided by the registered user to the corresponding identity verifier [column 11, lines 15-19];

receiving one of the plurality of identity verifiers from a requesting party, the requesting party having received the one identity verifier from a transaction initiator [column 11, lines 15-19];

determining whether the one identity verifier received from the requesting party is associated with a corresponding security message [column 27, lines 15-50]; and

transmitting to the requesting party an indication of whether the one identity verifier received from the requesting party is associated with a corresponding security message [column 27, lines 15-50].

As to claim 28, Flitcroft et al discloses that transmitting the message associated with the received identity verifier includes enabling the requesting party to compare the message pertaining to the transaction with a transaction initiated by the transaction initiator.

As to claim 29, Flitcroft et al discloses a method of protecting numerical identifiers associated with registered users, the method comprising:

obtaining at least one registered user;

obtaining a list for each registered user, each list including at least one numerical identifier, each numerical identifier included in the list associated with the registered user [column 9 line 64 to column 10 line 18];

obtaining at least two identity verifiers for each registered user, each identity verifier to be used in only one transaction [column 9 line 64 to column 10 line 18];

associating each of the at least two identity verifiers with the corresponding registered user [column 9 line 64 to column 10 line 18]; and

transmitting to each registered user the at least two identity verifiers associated with the registered user, each of the identity verifiers enabling the registered user to verify to a requesting party any the numerical identifier from the list [column 11, lines 15-19], and each of the identity verifiers capable of verifying the selected numerical identifier [column 11, lines 15-19].

As to claim 33, Flitcroft et al discloses a system for protecting numerical identifiers of registered users, the system comprising:

an input device configured to obtain a corresponding list for each of a plurality of registered users, each list including at least one numerical identifier, the input device being further configured to obtain at least two identity verifiers for each of the plurality of registered users [column 9 line 64 to column 10 line 18];

a database configured to associate each of the plurality of registered users with the corresponding list of the at least one numerical identifier, the database being further configured to associate each of the at least two identity verifiers with the corresponding registered user [column 9 line 64 to column 10 line 18]; and

a communications device configured to transmit to each registered user the at least two identity verifiers associated with the registered user [column 9 line 64 to column 10 line 18], each of the identity verifiers enabling the registered user to

verify to requesting parties any numerical identifier selected from the list by the registered user [column 9 line 64 to column 10 line 18], and each of the identity verifiers being capable of verifying the selected numerical identifier in any one transaction [column 11, lines 15-19].

As to claim 34, Flitcroft et al discloses a system of obstructing identity crimes, the system comprising:

an input device configured to obtain a list of at least two identity verifiers to be associated with a registered user [column 9 line 64 to column 10 line 18], the registered user selected from the group consisting of persons and entities, each identity verifier to be used for no more than one transaction, the input device further configured to enable the registered user to provide a security message to be associated with one of the identity verifiers [column 9 line 64 to column 10 line 18], the security message indicating information pertaining to an intended transaction [column 9 line 64 to column 10 line 18];

a database configured to link the list of identity verifiers to at least one numerical identifier associated with the registered user [column 11, lines 15-19], the database further configured to link a security message to one of the identity verifiers if the registered user has provided such a security message [column 11, lines 15-19];

a communication device configured to receive a numerical identifier and an identity verifier from a requesting party, the requesting party having obtained the numerical identifier and the identity verifier from a transaction initiator

claiming to be associated with the numerical identifier [column 11, lines 15-19], the communication device further configured to transmit to the requesting party information indicating whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier and whether a security message has been associated with the received identity verifier [column 27, lines 15-50]; and

a processing device configured to determine whether the received identity verifier is within the list of identity verifiers linked in the database to the received numerical identifier [column 27, lines 15-50], the processing device further configured to determine whether the received identity verifier is associated with a security message [column 27, lines 15-50].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flitcroft et al U.S. Patent No. 6,636,833 B1 as applied to claim 1 above, and further in view of Kuhns et al U.S. Patent No. 6,047,281.**

As to claim 5, Flitcroft et al does not teach storing public information about the registered user whose identity is to be verified. Flitcroft et al does not teach creating at least two categories of requesting parties. Flitcroft et al does not teach receiving instructions from the registered user

regarding what public information is allowed to be released to each of the at least two categories of requesting party. Flitcroft et al does not teach determining the category of the requesting party. Flitcroft et al does not teach communicating the appropriate public information to the requesting party pursuant to the instructions from the registered user.

Kuhns et al teaches storing public information about the registered user whose identity is to be verified [column 1, lines 22-38]. Kuhns et al teaches creating at least two categories of requesting parties. Kuhns et al teaches receiving instructions from the registered user regarding what public information is allowed to be released to each of the at least two categories of requesting party. Kuhns et al teaches determining the category of the requesting party [column 16, lines 1-46]. Kuhns et al teaches communicating the appropriate public information to the requesting party pursuant to the instructions from the registered user [column 17, lines 24-48].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Flitcroft et al so that there would have been public information stored about the registered user whose identity is to be verified. There would have been at least two categories created of requesting parties. The registered user would have sent messages regarding what public information is allowed to be released to each of the at least two categories of requesting party. The category of the requesting party would have been determined. The appropriate public information would have been sent to the requesting party pursuant to the instructions from the registered user.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Flitcroft et al by the teaching of Kuhns et al because it

helps eliminate fraud and protects the general public from individuals with criminal records [column 2, lines 30-50].

**8. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flitcroft et al U.S. Patent No. 6,636,833 B1 as applied to claim 1 above, and further in view of Shkedy U.S. Patent No. 6,236,972.**

As to claims 6 and 9, Flitcroft et al does not teach that the at least one numerical identifier is a social security number or a phone number.

Shkedy teaches an identifier being a social security number or a phone number [column 13, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Flitcroft et al so that the pseudorandom number would have been replaced by the social security number or the phone number of the user.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Flitcroft et al by the teaching of Shkedy because both of those numbers are unique and easily remembered [column 13, lines 16-29].

*Conclusion*

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy *AM*  
June 20, 2006

*Ayaz R. Sheikh*  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100